零基础入门　快速掌握软件应用

SO EASY TO LEARN!!

黑客攻防从新手到高手

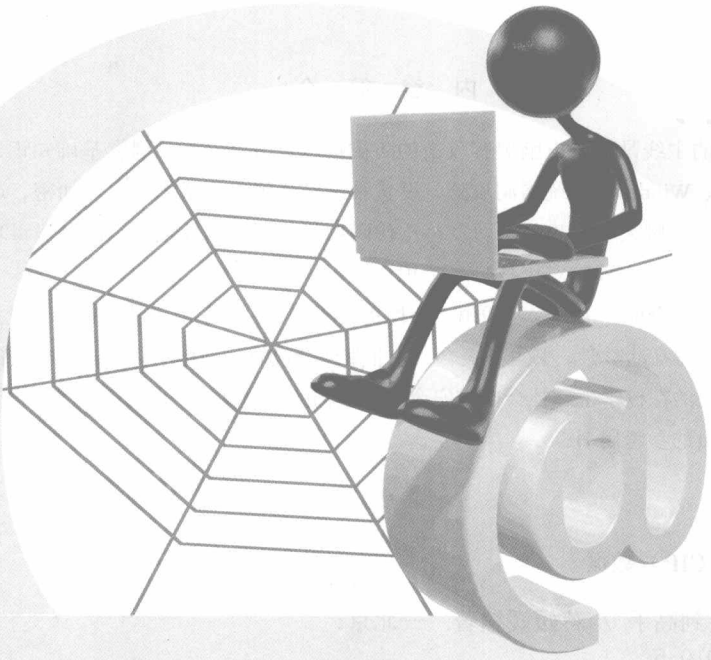
蒋媛媛　编著

1DVD 视频教学

- 精选50个精彩视频直播
- 6小时案例讲解全程再现
- 附赠《电脑常见故障诊断与排除从新手到高手》和《系统优化与故障排除从新手到高手》教学视频

- 采用全程图解的形式编写　可操作性强　立竿见影
- “全程图解教学+多媒体视频讲解”教学模式　轻松上手
- 超值光盘互动教学　书盘完美结合

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE



黑客攻防从新手到高手

蒋媛媛　编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 简 介

本书内容的主线是针对电脑黑客攻击的防御技术，内容涵盖了黑客基础知识、常用扫描与嗅探工具、Windows 系统漏洞攻防、设置系统安全策略、系统与文件加密、远程控制攻防、木马攻防、聊天软件攻防、网页恶意代码攻防、电子邮件攻防、U 盘病毒攻防、使用电脑安全软件、黑客攻防实用技巧等知识。

本书内容权威全面、讲解深入浅出，全程实战图解、注重学习方法，精心开设栏目、全新学习体验，光盘互动教学、书盘完美合一，非常适合没有任何电脑黑客攻防知识的初学者以及大中专院校的在校学生和社会电脑安全培训机构的学员使用，也可作为网络安全从业人员、网络管理员的参考用书。

图书在版编目（CIP）数据

黑客攻防从新手到高手 / 蒋媛媛编著. --北京：
中国铁道出版社，2010.5
ISBN 978-7-113-11246-2

Ⅰ.①黑… Ⅱ.①蒋… Ⅲ.①计算机网络－安全技术
Ⅳ.①TP393.08

中国版本图书馆 CIP 数据核字（2010）第 055273 号

书　　名：黑客攻防从新手到高手
作　　者：蒋媛媛　编著

责任编辑：苏　茜　　**编辑部电话：**（010）63560056
编辑助理：赵　鑫
封面设计：张　丽　　**封面制作：**白　雪
责任印制：李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街 8 号　　邮政编码：100054）
印　　刷：三河市华业印装厂
版　　次：2010 年 8 月第 1 版　　2010 年 8 月第 1 次印刷
开　　本：787mm×1092mm　1/16　**印张：**20　　**字数：**471 千
印　　数：4 000 册
书　　号：ISBN 978-7-113-11246-2
定　　价：39.80 元（附赠光盘）

Foreword 前言

编写简介

目前，互联网在不断地迅猛发展，给人们的生活提供了无限自由和大量财富，也为广大网民间的交流提供了极大方便。但是，与此同时互联网也带来了消极影响，“信息垃圾”、“邮件炸弹”、“电脑病毒”、“黑客入侵”等越来越威胁到网络的安全。尤其是电脑黑客攻击，现在已成为威胁网络安全的最大隐患。

本书旨在使读者了解黑客的攻击手段，使读者在实际网络应用中遇到黑客攻击时，能够最大限度地减少损害和损失。更为重要的是，希望读者能够运用本书介绍的攻防技术来防范黑客的恶意攻击，使自己的网络更加安全。

内容概述

本书的主线是电脑黑客的“攻”与“防”，每章基本上都是围绕这两点进行深入讲解的。内容涵盖黑客攻防工具和各种黑客攻防技术，并着重讲解了电脑安全软件的使用以及黑客攻防实战技巧等实用知识。

全书共分为 13 章，主要内容包括黑客基础知识、常用扫描与嗅探工具、Windows 系统漏洞攻防、设置系统安全策略、系统与文件加密、远程控制攻防、木马攻防、聊天软件攻防、网页恶意代码攻防、电子邮件攻防、U 盘病毒攻防、使用电脑安全软件、黑客攻防实用技巧等知识。

本书特色

每个初学者都想通过最行之有效的学习方法、最简洁易懂的讲解方式尽可能多地掌握电脑操作技能和技巧，本书将是您最好的选择。本书由资深电脑教育专家精心策划编写而成，主要具有以下特色：

内容全面权威、讲解深入浅出：针对电脑初学者，内容涵盖电脑黑客攻防的各个方面，权威全面、循序渐进，讲解清晰明了、深入浅出，让读者一看就懂，一练就会。

全程实战图解、注重学习方法：采用全程图解的形式组织编写，简便直观、可操作性强，并注重培养读者正确、高效的学习方法，达到立竿见影的学习效果。

全新教学模式、提升实战技能：采用“全程图解教学+多媒体视频讲解”的模式，并以图解标注突出讲解关键性操作步骤，使读者轻松掌握实战操作技能，即学即用。

光盘互动教学、书盘完美合一：超长全新的多媒体互动学习光盘，囊括全书重要知识点和所有实战操作的全程教学视频或课件，为读者提供了一套生动鲜明的“活教材”。

适用读者

本书适用面广，主要适合以下读者群体学习使用：

（1）没有任何电脑黑客攻防知识的初学者；

（2）对电脑黑客攻防技术有些了解但不精通的学习者；

（3）网络安全从业人员以及网络管理员；

（4）大中专院校的在校学生和社会电脑安全培训机构的学员；

（5）想在短时间内全面掌握电脑安全实用技能的读者朋友。

售后说明

如果读者在使用本书的过程中遇到什么问题或者有什么好的意见或建议，可以通过发送电子邮件（E-mail：jtbook@yahoo.cn）或者在线（QQ：843688388）联系我们，我们将及时予以回复，并尽最大努力提供学习上的指导与帮助。

希望本书能对广大读者朋友提高学习和工作效率有所帮助，由于编者水平有限，书中可能存在不足之处，欢迎读者朋友提出宝贵意见，我们将加以改进，在此深表谢意！

特别提醒

根据国家有关法律规定，任何入侵和窃取他人系统和文件的做法都是违法的，希望读者不要使用本书介绍的黑客技术攻击他人电脑，否则后果自负，特此声明！

编　者

2010 年 3 月

目 录

07 木马攻防

08 聊天软件攻防

09 网页恶意代码攻防

10 电子邮件攻防

11 U 盘病毒攻防

12 使用电脑安全软件

Chapter 01

黑客基础知识

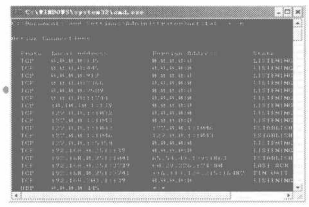
随着网络技术的不断发展，人们的日常生活和工作越来越离不开网络，互联网给我们带来了极大便利，但随之出现的网络安全问题也成为用户最为头痛的事情。在学习黑客攻防技术之前，首先我们来了解一些关于黑客的基础知识，认识 IP 地址、端口和一些黑客常用的 DOS 命令，最后创建一个安全的测试环境。

本章建议学习时间：

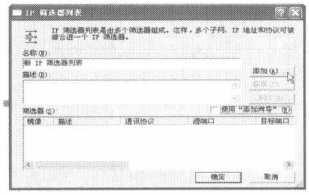
本章建议学习时间为 50 分钟，其中分配 15 分钟学习黑客、IP 地址和端口基础知识，15 分钟了解黑客常用的命令，20 分钟用于学习创建安全的测试环境。

学完本章后您可以：

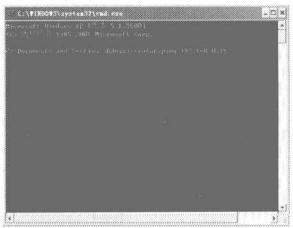
- 了解黑客的行为
- 认识 IP 地址
- 认识端口
- 了解黑客的常用命令
- 创建安全的测试环境



查看端口状态



IP 筛选器列表



输入 ping 命令

DVD 重要知识点视频索引

1.1 揭开黑客的神秘面纱

谈到网络安全，人们不自觉地就会联想到黑客，人们往往会将他们同破坏网络安全、盗取用户账号、偷窃个人私密信息等行为联系起来。其实黑客也有好坏之分，他们并不全是网络上的捣乱分子，其中也有一部分是网络上的安全卫士。下面我们就来揭开黑客的神秘面纱，让用户详细了解黑客到底是一群什么样的人。

在黑客圈中，Hacker 一词早期是带有正面意义的，但到了今天，“黑客”一词已经成为那些专门利用电脑进行破坏或入侵他人电脑的人的代名词，其实对这种人正确的叫法应该是 Cracker，有人翻译成“骇客”。也正是由于这些人的出现玷污了“黑客”一词，使人们把黑客和骇客混为一体。黑客和骇客根本的区别是：黑客们修补系统漏洞，而骇客们利用系统漏洞进行破坏。

1.1.1 黑客的兴起

黑客最早出现于 20 世纪 50 年代，最早的计算机于 1946 年在宾夕法尼亚大学出现，而最早的黑客则出现于麻省理工学院，贝尔实验室也有。最初的黑客一般都是一些高级的技术人员，他们热衷于挑战、崇尚自由，并主张信息的共享。

1994 年以来，因特网在全球的迅猛发展为人们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，信息已成为物质和能量以外维持人类社会的第三资源，它是未来生活中的重要介质。随着电脑的普及和因特网技术的迅速发展，现代意义上的黑客也随之出现。

“黑客”一词一般有以下四种意义：

❖ 一个对（某领域内的）编程语言有足够了解，可以不经长时间思考就能创造出有用的软件的人。

❖ 一个试图恶意（一般是非法地）破解或破坏某个程序、系统及网络安全的人。这个意义常常对那些符合上个条件的黑客造成严重困扰，他们建议媒体将这群人称为“骇客”。

❖ 一个试图破解某系统或网络，以提醒该系统所有者及其电脑系统的安全漏洞，这群人往往被称做“红客”。许多这样的人是电脑安全公司的雇员，并在完全合法的情况下攻击某系统。

❖ 一个通过知识或猜测而对某段程序做出（往往是好的）修改，并改变（或增强）该程序用途的人。

现在，网络上出现了越来越多的 Cracker，他们只是入侵，使用扫描器到处乱扫，用 IP 炸弹轰炸，毫无目的地入侵、破坏，他们并无益于电脑技术的发展，反而有害于网络的安全，造成网络瘫痪，给人们带来巨大的经济和精神损失。

1.1.2 黑客的组成

到了今天，黑客已经不像以前那样是少数现象，他们已经发展成网络上的一个独特的群

体。他们有着与常人不同的思维方法，有着自己独特的行为方式，网络上现在出现了很多由一些志同道合的人组织起来的黑客组织。但是这些人是从什么地方来的呢？他们是什么样的人？其实除了极少数的职业黑客以外，大多数黑客都是业余的，而黑客其实和现实中的平常人没有区别，或许他就是一个普通的高中在读学生。

有人曾经对黑客年龄这方面进行过调查，组成黑客的主要群体是 18~30 岁之间的年轻人，大多是男性，不过现在有很多女性也加入到这个行列。他们大多是在校的学生，因为他们有着很强的电脑爱好和很多自由时间，好奇心强、精力旺盛等使他们步入了黑客的行列。还有一些黑客有自己的事业或工作，包括程序员、资深安全员、安全研究员、职业间谍、安全顾问等。当然这些人的技术水平与刚刚入门的“小黑客”无法相比，不过他们也是从新手一步步地走过来的。

1.1.3 黑客的主要行为

“黑客”大体上应该分为“正”、“邪”两类，正派黑客依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并加以完善；邪派黑客则是通过各种黑客技能对系统进行攻击、入侵或者做其他一些有害于网络的事情。

无论哪类黑客，他们最初的学习内容都是本书所涉及的内容，而且掌握的基本技能也都是一样的。即便日后他们各自走上了不同的道路，但是所做的事情也差不多，只不过出发点和目的不一样而已。

黑客的行为主要有以下几种：

其一，学习技术。互联网上的新技术一旦出现，黑客就立刻学习，并用最短的时间掌握这项技术。这里所说的掌握并不是一般的了解，而是阅读有关的“协议”、深入了解此技术的机理。一旦停止学习，那么依靠他以前掌握的内容，并不能维持他的“黑客”身份超过一年。

其二，伪装自己。黑客的一举一动都会被服务器记录下来，所以黑客都会伪装自己，使得对方无法辨别其真实身份。这需要熟练的技巧，还有用来伪装自己的 IP 地址、使用跳板逃避跟踪、清理记录扰乱对方线索、巧妙躲开防火墙等。

伪装是需要非常过硬的基本功才能实现的，初学者不可能在短时间内学会。

其三，发现漏洞。漏洞对黑客来说是最重要的信息，黑客要经常学习别人发现的漏洞，并努力自己寻找未知漏洞，并从海量的漏洞中寻找有价值的、可被利用的漏洞进行试验。当然，他们最终的目的是通过漏洞进行破坏或者修补上这个漏洞。

其四，利用漏洞。对于正派黑客来说，漏洞要被修补；对于邪派黑客来说，漏洞要用来搞破坏。

作为一名黑客，道德是非常重要的，这往往决定一个黑客的前途和命运。如果开始学习的时候就是为了扬名或非法获利，那就不能称之为黑客。但是，虚拟的网络世界不能用现实中的规范去管理，而黑客又是在这个虚拟世界里最渴望自由和共享的。虽然网络上的黑客道德或守则出现很多，也有很多黑客章程，但是这些所谓的道德往往成为一纸空文，黑客们真正遵守的是来自内心真诚的道德，是一种信仰，而不是人为的、外在的一种守则。也只有这些来自于黑客们内心的道德才可以真正地约束他们。

现在有不少人以盗取他人的游戏账号、银行卡号，窃取公司机密，攻击别人网站，敲诈，

欺骗等非法获利，这些人都不能称之为“黑客”，对于他们应该称为“骇客”更为合适，他们最终会受到法律的制裁和良心的谴责。

1.2 认识 IP 地址

用户都知道，在我们常用的电话通信中，电话用户是靠电话号码来识别的。同样，在网络中为了区别不同的计算机，也需要给计算机指定一个号码，这个号码就是“IP 地址”。下面一起来认识一下 IP 地址。

1.2.1 IP 地址的表示方法

IP 地址就像是我们的家庭住址一样，如果你要写信给一个人，你就要知道他（她）的地址，这样邮递员才能把信送到。计算机发送信息时就好像邮递员，它必须知道唯一的“家庭地址”才不至于把信送错人家。所不同的是，我们的地址使用文字来表示，而计算机的地址用二进制数字表示。

IP 地址的长度为 32 位，分为 4 个字节，每个字节对应 8 位二进制位，即每部分数字不超过 2^8=256。例如，一个用二进制形式记录的 IP 地址可以表示为：11000000 10011110 00000011 00000101。

为了方便使用，IP 地址的每个字节通常用十进制形式表示，每段数字范围为 0～255，段与段之间用句点隔开，如上面的 IP 地址就可以表示为：192.158.3.5。IP 地址的这种表示方法叫做“点分十进制表示法”，这显然比大量 1 和 0 容易记忆得多。

1.2.2 IP 地址的分类

最初设计互联网络时，为了便于寻址以及层次化构造网络，每个 IP 地址分为网络地址和主机地址两部分。同一个物理网络上的所有主机都使用同一个网络地址，而同一网络上的一个主机都有一个主机地址与其对应。

IP 地址根据网络 ID 的不同分为 5 种类型，即 A 类地址、B 类地址、C 类地址、D 类地址和 E 类地址。

1．A 类 IP 地址

一个 A 类 IP 地址由 1 字节的网络地址和 3 字节主机地址组成，网络地址的最高位必须是“0”，地址范围为：1.0.0.1～126.255.255.254（二进制表示为：00000001 00000000 00000000 00000001～01111110 11111111 11111111 11111110）。可用的 A 类网络有 126 个，每个网络能容纳 1 677 214 台主机。

2．B 类 IP 地址

一个 B 类 IP 地址由 2 字节的网络地址和 2 字节的主机地址组成，网络地址的最高位必须是“10”，地址范围为：128.1.0.1～191.255.255.254（二进制表示为：10000000 00000001 00000000 00000001～10111111 11111111 11111111 11111110）。可用的 B 类网络有 16 384 个，每个网络能容纳 65 534 台主机。

3．C 类 IP 地址

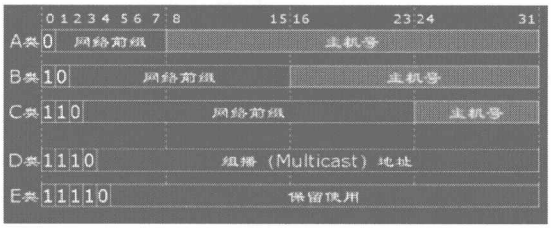
一个 C 类 IP 地址由 3 字节的网络地址和 1 字节的主机地址组成，网络地址的最高位必须是 110，地址范围为 192.0.1.1～223.255.255.254（二进制表示为：11000000 00000000 00000001 00000001～11011111 11111111 11111111 11111110）。C 类网络可达 2 097 152 个，每个网络能容纳 254 个主机。

4．D 类 IP 地址

D 类 IP 地址第一个字节以 1110 开始，地址范围为：224.0.0.1～239.255.255.254。它是一个专门保留的地址，并不指向特定的网络，目前这一类地址被用在多点广播（Multicast）中。多点广播地址用来一次寻址一组计算机，它标识共享同一协议的一组计算机。

5．E 类 IP 地址

E 类地址仅作实验和将来开发而保留，它以 1111 开始，全 0（0.0.0.0）的 IP 地址指任意网络，全 1 的 IP 地址（255.255.255.255）是当前子网的广播地址，如下图所示。



1.3 认识端口

计算机“端口”（port）可以认为是计算机与外界通信交流的出口，其中硬件领域的端口又称接口，如 USB 端口、串行端口等；软件领域的端口一般指网络中面向连接服务和无连接服务的通信协议端口，是一种抽象的软件结构，包括一些数据结构和 I/O（基本输入/输出）缓冲区。

在网络技术中，端口（port）有多种含义。集线器、交换机、路由器的端口指的是连接其他网络设备的接口，如 RJ-45 端口、Serial 端口等。这里所指的端口不是物理意义上的端口，而是特指 TCP/IP 协议中的端口，是逻辑意义上的端口。

如果把 IP 地址比作一间房子，TCP/IP 协议中的端口指的就是出入这间房子的门。真正的房子只有几个门，但是一个 IP 地址的端口可以有 65 536（即 256×256）个。端口是通过端口号来标记的，端口号只有整数，范围是 0～65 535（256×256－1）。

1.3.1 端口的分类

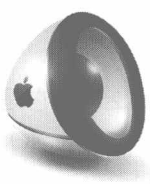
计算机中的端口按不同的标准可以分为很多类，其中最常用的分类标准有以下两种：

1．按端口号分布划分

按端口号分布划分，可以将端口分为三大类，分别为：公认端口、注册端口和动态/私有端口。

（1）公认端口

公认端口是指那些用户所熟知的端口号，范围为0～1023，它们紧密绑定于一些服务。通常这些端口的通信明确表明了某种服务的协议。例如，80端口分配给WWW服务，21端口分配给FTP服务等。



提示

我们在IE浏览器的地址栏中输入一个网址的时候是不必指定端口号的，因为在默认情况下WWW服务的端口号是80。

（2）注册端口

注册端口（registered ports）的端口号为1024～49151。它们松散地绑定于一些服务，也就是说有许多服务绑定于这些端口，这些端口同样用于许多其他目的。这些端口大多数没有明确的定义服务对象，应用程序可以根据自己的需要进行定义。例如，我们常用的聊天软件腾讯QQ用的就是4000端口。

（3）动态/私有端口

动态/私有端口（dynamic/private ports）的端口号为49152～65535。理论上，不应为服务分配这些端口。但实际上一些较为特殊的程序，特别是一些木马程序常常使用这些端口，因为它们通常从1024起分配动态端口而不被人们注意，容易隐藏，如SUN的RPC端口就是从32768端口开始的。

2．按通信服务方式划分

计算机通信的连接方式有以下两种：

第一种是直接与接收方进行的连接，发送信息以后，可以确认信息是否到达，这种方式大多采用TCP协议。

第二种是不直接与接收方进行连接，只管把信息放在网上发出去，而不管信息是否到达，也就是“无连接方式”。这种方式大多采用UDP协议，IP协议也是一种无连接方式。

对应使用以上这两种通信协议的服务所提供的端口，也就分为“TCP协议端口”和“UDP协议端口”。计算机之间相互通信一般采用这两种通信协议。

使用TCP协议的常见端口主要有以下几种：

❖ FTP：定义了文件传输协议，使用21端口。用户常说某计算机开启了FTP服务，便是启动了文件传输服务，下载文件、上传主页都要用到FTP服务。

❖ Telnet：它是一种用于远程登录的端口，用户可以以自己的身份远程连接到计算机上，通过这种端口可以提供一种基于DOS模式下的通信服务。早期的BBS是纯字符界面，支持BBS的服务器将23端口打开，对外提供服务。

❖ SMTP：定义了简单邮件传送协议，现在很多邮件服务器用的都是这个协议，用于发送邮件。常见的免费邮件服务用的就是这个邮件服务端口，所以在电子邮件设置中常看到有SMTP端口设置栏，服务器开放的是25端口。

❖ POP3：它和SMTP对应，POP3用于接收邮件。通常情况下，POP3协议所用的是110端口。也就是说，只要有相应的使用POP3协议的程序（如Foxmail或Outlook），就可以不以

Web 方式登录邮箱界面，直接用邮件程序就可以收到邮件（如果是 163 邮箱就没有必要先进入网易网站，再进入自己的邮箱来收信）。

使用 UDP 协议的端口常见的有：

❖ HTTP：这是用户用得最多的协议，它就是常说的“超文本传输协议”。上网浏览网页时，就得在提供网页资源的计算机上打开 80 端口以提供服务，常见的“WWW 服务”、“Web 服务器”用的就是这个端口。

❖ DNS：用于域名解析服务，这种服务在 Windows NT 系统中用得最多。因特网上的每一台计算机都有一个网络地址与之对应，这个地址就是常说的 IP 地址，它以纯数字+“.”的形式表示。然而这不便记忆，于是出现了域名，访问计算机的时候只需要知道域名，域名和 IP 地址之间的变换由 DNS 服务器来完成。DNS 用的是 53 端口。

❖ SNMP：简单网络管理协议，使用 161 端口，用来管理网络设备。由于网络设备很多，无连接的服务就体现出其优势。

❖ QQ：QQ 程序既接受服务，又提供服务，这样两个聊天的人才是平等的。QQ 用的是无连接的协议，也就是说它用的是 UDP 协议。QQ 服务器使用 8000 端口，侦听是否有信息到来，客户端使用 4000 端口，向外发送信息。如果上述两个端口正在使用（有很多人同时和几个好友聊天），就顺序往上加。

另外，代理服务器常用以下端口：

❖ HTTP 协议代理服务器常用端口：80/8080/3128/8081/9080。

❖ SOCKS 代理协议服务器常用端口：1080。

❖ FTP 协议代理服务器常用端口：21。

❖ Telnet 协议代理服务器常用端口：23。

1.3.2 查看系统的开放端口

通过了解系统开放端口的状态变化，可以帮助我们更好地保护系统、防范黑客入侵、保证电脑安全。用户可以使用 netstat 命令查看自己系统端口的状态，了解系统当前开放了哪些端口。使用 netstat 命令查看系统端口的具体操作步骤如下：

STEP 01 打开“运行”对话框

单击“开始”|“运行”命令，打开“运行”对话框，如下图所示。

STEP 02 输入 cmd 命令

在“打开”下拉列表框中输入 cmd 命令，然后单击“确定”按钮，打开“命令提示符”窗口，如下图所示。